International Conference on Interdisciplinary Research in Electronics and Instrumentation Engineering 2015 [ICIREIE 2015]

ISBN	978-81-929866-3-0		**VOL**	01
Website	www.icireie.org		**eMail**	icireie@asdf.res.in
Received	10 - July - 2015		**Accepted**	31- July - 2015
Article ID	ICIREIE010		**eAID**	ICIREIE.2015.010

Hash based Secure Multicast Routing in Mobile Ad Hoc Network

P Vigneshwaran[1], R Dhanasekaran[2]
[1]Associate Professor, Department of Information Technology,
Rajalakshmi Institute of Technology, Chennai, Tamilnadu, India
[2]Professor, Department of Electrical and Electronics Engineering,
Syed Ammal Engineering College, Ramanathapuram, Tamilnadu, India

Abstract: *Mobile Ad Hoc Network (MANET) consists of number of mobile nodes which follows a dynamic topology. In Nodes in MANET moves in an undefined manner and each node is acted as a mobile router. In this dynamic architecture, a malicious node is capable of disrupting the routing messages by refusing to forward routing messages, or it can inject the wrong routing packets and also modifies routing information. Hence security is a major concern in MANET. In this paper, we have proposed a secure multicast routing protocol based on secret sharing with double hash functions to overcome insider and outside attack. Keys are generated and it is transmitted via the secured medium using secret sharing (SS) method. Based on the shares generated by the source using the SS, hash values are calculated and it is appended to the share. The receivers of the intended data transmission retrieve all the shares and apply the hash function to recover each share. The proposed scheme is compared with the ODMRP and other existing approaches using NS2. Based on the simulation, we have obtained the better results in terms of high packet delivery ratio with reduced network load and control overhead.*

Keywords: Confidentiality, Authentication, ODMRP, secret sharing, MANET, hash function

I. INTRODUCTION

A Mobile Ad-hoc NETwork or MANET is defined as a wireless network of mobile nodes communicating with each other in a multi-hop fashion without the support of any fixed infrastructure. The term Ad hoc implies that this network is a special network that is established to provide a special, often extemporaneous service customized to specific applications. In MANET, routing and resource managements are done in a distributed manner: that is, all nodes coordinate with other nodes to enable communications among themselves. This requires each node to be more knowledge so that it can operate both transmitting and receiving data. Establishing communication among a group of soldiers in a battle field is a good example. Another area in which MANET can be deployed is collaborative and distributed computing. The requirement for a temporary communication network among a group of people in a conference, meeting or classrooms necessitates the formation of mobile ad-hoc network. For example, consider a group of researchers who want to share their research presentations during a conference. In such case, the formation of a mobile ad-hoc network with the necessary support for multicast routing can serve the purpose. These distributed file sharing applications will not require the level of

Cite this article as: P Vigneshwaran, R Dhanasekaran. “Hash based Secure Multicast Routing in Mobile Ad Hoc Network.” *International Conference on Interdisciplinary Research in Electronics and Instrumentation Engineering (2015)*: 55-60. Print.

security expected in a military environment. Security aspects such as data integrity and data protection against unauthorized access are still compromised. Security in ad-hoc wireless networks is very important. The lack of any central administration makes MANET more vulnerable to attacks than wired networks.

Multicast means being able to deliver a packet to a group of receivers. The typical applications of multicast are multi-party video or audio conferencing, resource discovery, news feeds, online games, television, video transmission etc., Several multicast routing algorithms have been proposed for MANET to achieve the goal. Security in multicast is considered as more complicated than in the unicast operation. Mobile ad-hoc networks, due to their unique characteristics, are generally more vulnerable to information and physical security threats than wired networks or infrastructure based wireless networks. The ultimate goal of the security solutions for MANET is to provide security services such as authentication, confidentiality, integrity, availability and nonrepudiation to mobile users. In order to achieve this goal, the security solution should provide complete protection spanning over the entire protocol stack. There is no single mechanism that will provide all the security services in MANET.

II. RELATED WORKS

MANETs have certain challenges in security due to its characteristics. The main requirement to is ensure the security in MANET to have a secure routing protocol which should have properties to detect the behavior of the mobile nodes, guarantee of exact route discovery process, maintaining confidential network topological information and to be self-stable against attacks. Hu et al proposed [1] a secure ad hoc routing protocol based on the design of the DSDV routing protocol. It used a efficient one-way hash function that support use with nodes of limited CPU processing capability and to guard against DOS attack. SEAD is efficient and can be used in networks of computation- and bandwidth-constrained nodes. SEAD actually outperforms DSDV-SQ in terms of packet delivery ratio, although it does create more overhead in the network, both due to an increased number of routing advertisements it sends, and due to the increase in size of each advertisement due to the addition of the hash value on each entry for authentication. Gonzalez et al [2] proposed mechanism that enables the detection of nodes that exhibit packet forwarding misbehavior. The proposed algorithm does not require high density networks in which many nodes can overhear each other's received and transmitted packets. The simulation shown that it can detect the nodes that misbehave by dropping a significant percentage of packets. Yang et al [3] proposed a SCAN, a unified network-layer security solution for such networks that protects both routing and data forwarding operations through the same reactive approach. SCAN does not apply any cryptographic primitives on the routing messages. Instead, it protects the network by detecting and reacting to the malicious nodes. In SCAN, local neighboring nodes collaboratively monitor each other and sustain each other, while no single node is superior to the others. SCAN also adopts a novel credit strategy to decrease its overhead as time evolves. In essence, SCAN exploits localized collaboration and information cross-validation to protect the network in a self-organized manner. The proposed design is self-organized, distributed, and fully localized. Both analysis and simulations results have confirmed the effectiveness and efficiency of SCAN in protecting the network layer in mobile ad hoc networks.

Khurana et al [4] proposed a simple and efficient algorithm to solve the routing problems in misbehaving nodes. It does not address the problem of handling attack directly but tries to minimize the impact of the attack. Yu et al [5] proposed a novel algorithm that detects internal attacks during route discovery. The route-discovery messages are protected by pairwise secret keys between a source and destination and some intermediate nodes along a route established by using public key cryptographic mechanisms. They also proposed an optimal routing algorithm with routing metric combining both requirements on a node's trustworthiness and performance. A node builds up the trustworthiness on its neighboring nodes based on its observations on the behaviors of the neighbor nodes. Both of the proposed algorithms can be integrated into existing routing protocols for MANETs, such as ad hoc on-demand distance vector routing (AODV) and dynamic source routing (DSR). As an example, we present such an integrated protocol called secure routing against collusion (SRAC), in which a node makes a routing decision based on its trust of its neighboring nodes and the performance provided by them. The simulation results have demonstrated the significant advantages of the proposed attack detection and routing algorithm over some known protocols. ARIADNE is a well-known secure on-demand ad hoc network routing protocol, which proposes a mechanism to avoid routing attacks and DoS attacks [6]. Wadbude et al [7] proposed approach uses improved of security mechanisms to introduce in the proposed techniques so that it satisfies the main security requirement and guarantees the discovery of a correct and secure route. The security mechanisms that the protocol uses are the hash chain, digital signature and Protocol Enforcement Mechanism. Rajesh Babu et al. [8] have proposed to develop an energy efficient secure authenticated routing protocol (EESARP).

Poonam Yadav et al. [9] have introduced the on-demand routing protocols AODV, DSR and DYMO based on IEEE 802.11 and the characteristic summary of these routing protocols are presented. Feng He et al. [10] have proposed a novel secure routing protocol S-MAODV which is based on MAODV. Kalpana et al. [11] have addressed anonymity and trust issues for a wireless network containing selfish and malicious nodes. Mike Burmester et al. [12] have analyzed provable secure route discovery algorithm which is vulnerable to a hidden channel attack. Stefaan Seys et al. [13] have studied anonymous routing protocol for mobile ad hoc networks. K.Seshadri Ramana et al. [14] have proposed a routing protocol that is based on securing the routing information from unauthorized users. Sridhar Subramanian et al. [15] have examined a trust based reliable protocol TBRAODV.Vigneshwaran et al [16] proposed an anomaly detection scheme based on a dynamic leaning process that allows the training data to be updated at particular time intervals. The dynamic learning process involves calculating the projection distances based on multidimensional statics using weighted coefficients and a forgetting curve. It uses ant colony optimization for detecting misbehavior nodes to prevent the behavior in between the path during the data transmission. Vigneshwaran et al [17] proposed a secure multicast routing protocol based on the SS. Multicast sender generates the shares and it is encrypted with keys generated by the KGC. Upon receiving the shares the multicast receivers performs the same interpolating polynomial operation to get the original data. Vigneshwaran et al [18] proposed an intelligent anomaly detection method using neural network algorithms to classify the behavior of the node based on the certain security parameters. The back propagation based learning strategy was used for classifying the node depends upon its behavior. The routing with intelligence have made the data traffic hassle free.

III. PROPOSED SYSTEM

Based on the architecture of MANET, every node in the MANET is having the unique address. In a network, any node is acting as a source and destination remaining all other nodes in the region is to be considered as routers. ODMRP is source initiated routing; we assumed that any request made by the source node to join the group is assumed to be genuine node. And also assume that every node in the network is having a public key which is known to others. The main aim of the proposed system is to transfer the data in a secured way to the group of receivers. The proposed system uses an authentication to identify the intended nodes for the data transmission. During the process of route discovery source node initiates the JOIN_QUERY and that is flooded in the network. Once the JOIN_QUERY is received by the nearby node should generate the routing table and update its information to the JOIN_QUERY and flooded in the rest of the network. Upon receiving the JOIN_QUERY packet the receiver nodes initiates the JOIN_REPLY based on the reverse path mechanism. During the process of JOIN_QUERY every node in the dynamic network is maintained its own routing table. A routing table is created on demand and is maintained by each node. The node creates an entry in the routing table only when a non-duplicate Join Query is received. The node stores the destination and the next hop to the destination. The routing table provides the next hop information when transmitting Join Replies. If two or more JOIN_QUERY is received by the same node, then a node selects a JOIN_QUERY packet with latest or recent sequence number. When a JOIN_QUERY packet reaches the multicast receiver, it creates and broadcasts a JOIN_REPLY to its neighbors.

When a node receives a JOIN_REPLY, it checks if the next node address of one of the entries matches its own address. If it does, the node realizes that it is on the path to the source and thus is part of the forwarding group; it sets the FG_FLAG (Forwarding Group Flag). It then broadcasts its own JOIN_REPLY to the network. The next node address field is filled in by extracting the information from its routing table. This way, the JOIN_REPLY is propagated by each forward group member until it reaches the multicast source via the selected path. The JOIN_REPLY packet consists of group of nodes associated with the transmission. Now the source node generates a group key request to the KGC based on the nodes presented in the JOIN_REPLY. All the nodes intended for the data transmission are received the group key from the KGC. The group of receiver node generates random challenges to the multicast source and that is transmitted to the KGC for preparing the shares. Now the KGC prepared the shares based on the received random challenge values and it computes f(x) and calculates the hash values. Now the f(x) and hash values are transmitted to the multicast source. If any node from the outside of the network may not have the sufficient knowledge the polynomial function f(x). Upon receiving the f(x), the outside node in the network are not in the position to recover the original messages. In that way the outsider attack is eliminated. The figure 1 shows the proposed system architecture. In our protocol, KGC communicates with the source S and shares a secret, with each receiver R_i during registration. For distributing a secret group key involving the receivers, KGC needs to broadcast a message containing (t+1) elements to all receivers. At the same time, each receiver needs to compute an interpolating polynomial f(x) to decrypt the secret group key. Thus, our proposed protocol is only suitable for distributing secret group key to a minimum number of receivers. After decrypting the secret key, the receivers are calculated the hash function for the received shares using secure hash algorithm 3. Now the receiver is having two hash values such as 1) calculated hash value 2) received hash value. Insiders and outsiders attack are acknowledged by comparing two hash values by the receiver. If there is any alteration in the hash value the received share is altered or modified by the attacker. To identify the replay attack, every share is enclosed with the Timestamp (T).

Algorithm:

Step 1: After the route discovery process, the multicast Source sends a request to the KGC for generating group keys.
Step 2: KGC generates a group key response with the list of receivers and transferred it to the multicast sender.
Step 3: Multicast receivers associated with the respective communication generates a random challenges and transmits it to the sender for manipulating the shares.
Step 4: KGC generates a group key based on the random challenges and it generates a share based on the polynomial function f(x) for all shares. KGC also computes the hash function for all the shares.
Step 5: Multicast source computes another hash function using SHA3 based on the polynomial function and already calculated hash value.
Step 6: For each multicast receiver computes the hash function based on SHA3 and generates a f(x) and hash value. Multicast receiver applies the reverse side of the polynomial functions to recover the original messages.

To calculate the new hash value receiver uses the same hash algorithm. If any attacker or third party affected the share, hash values does not match it. In such a way insider and outsider attacks are prohibited.

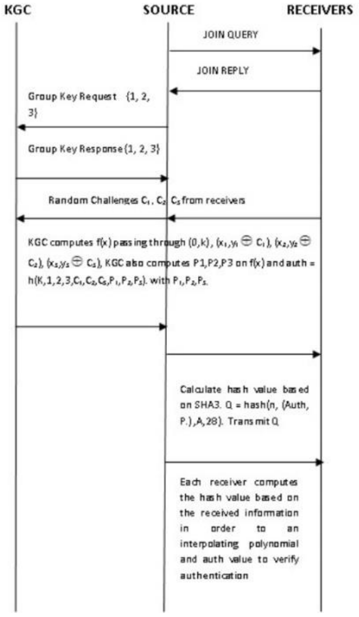
KGC
SOURCE
RECEIVERS
JOIN QUERY
JOIN REPLY
Group Key Request {1, 2, 3}
Group Key Response{1, 2, 3}
Random Challenges C_1, C_2, C_3 from receivers
KGC computes f(x) passing through (0,k), $(x_1,y_1 \ominus C_1)$, $(x_2,y_2 \ominus C_2)$, $(x_3,y_3 \ominus C_3)$, KGC also computes P1,P2,P3 on f(x) and auth = h(K,1,2,3,C_1,C_2,C_3,P_1,P_2,P_3). with P_1,P_2,P_3.
Calculate hash value based on SHA3. Q = hash(n, (Auth, P.),A,28). Transmit Q
Each receiver computes the hash value based on the received information in order to an interpolating polynomial and auth value to verify authentication

Figure 1. Architecture of proposed system

IV. RESULTS AND DISCUSSION

Our proposed approach is simulated in Network Simulator 2. The overall aim of the simulation study is to analyze the performance of the proposed system under the range of various parameters shown in Table 1. A pause time of 0 sec represents a network with very high mobility where all the nodes move continuously.

TABLE 1
SIMULATION ENVIRONMENT

Area	1000 m * 1000 m
MAC Protocol	IEEE 802.11 DCF
Wireless Channel	Free Space Propagation Model
Number of nodes	5,10,15,20,25,30,35,40,45,50
Traffic type	Constant Bit Rate
Mobility Model	Random way point
Mobility Speed	20 ms
Radio range	250 m
Simulation Time	50 ms
Initial energy of the node	1500 joules
Packet Size	Default size (512 Bytes)
Channel capacity	2 Mbps
Route refresh time	5 seconds

The proposed system is compared with other existing secure multicast routing protocol based on Network Load and Control Overhead. Based on the experimental results, we have obtained 5 to 10 % reduced control overhead and less network load compared with the existing approaches.

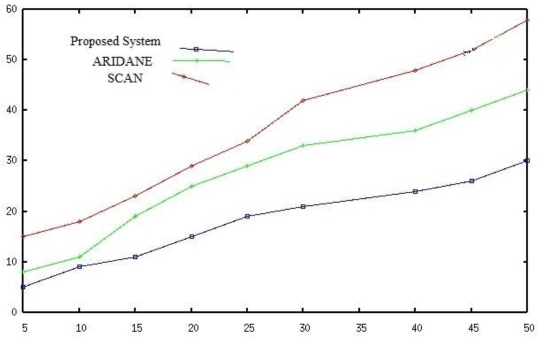

Figure 2. Control overhead

Cite this article as: P Vigneshwaran, R Dhanasekaran. "Hash based Secure Multicast Routing in Mobile Ad Hoc Network." *International Conference on Interdisciplinary Research in Electronics and Instrumentation Engineering (2015)*: 55-60. Print.

It is observed from figure 2 & 3, our proposed system produced less control overhead and utilizes less bandwidth compared to the other secure routing schemes. Even though, our proposed model performs of both encryption and an authentication for the shares, it produces less control overheads due to the fast cryptographic hash function. SHA3 is fast and secure hash algorithm and the time taken to perform the computation is too low when compared to the other hash functions such as SHA – 1, SHA - 2. Any one of the node in the network or outside of the network could notable to modify the routing data and message due to the Timestamp and hash value. SHA-3 provides a new security tool for system and protocol designers, and that may create opportunities for security in networks that did not exist before.

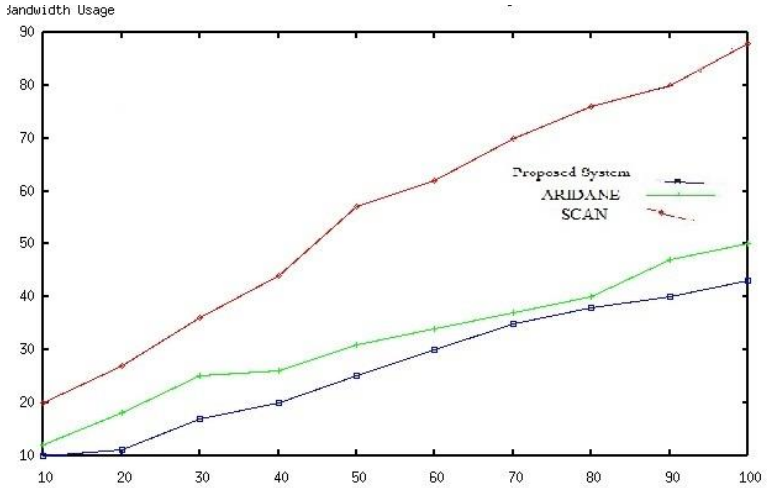

Figure 3. Bandwidth Utilization

V. CONCLUSION

We have proposed a secure multicast routing protocol based on double hashing. The source communicates with KGC to distribute the group key to all receivers. The confidentiality of our group key distribution is information theoretically secure. We provided a key authentication to identify whether the packets are transmitted and received by the authorized source and receivers. Key authentication is provided through the value of hash functions. Since the group key is known only to authorized receivers and KGC, unauthorized receivers cannot forge this value. In addition to that, another secure hash function is also applied to the calculated Auth value using the SHA3. Any insider node cannot forge a group key without being detected since the group key is a function of the secret shared between each receiver and KGC via source. In addition, any replay of the secret shares in step 4 can be detected since the group key is a function of each receiver random challenge. In our protocol, we only focus on protecting group key information broadcasted from KGC to all receivers. The insiders and outsiders attack have been identified and prevented. The simulation results have turned up effectively while considering the network load and control overhead and it produced less computation time compared to the existing systems.

REFERENCES

[1] Y.-C. Hu, D.B. Johnson, and A. Perrig, "SEAD: Secure Efficient Distance Vector Routing for Mobile Wireless Ad hoc Networks," Journal of Ad Hoc Networks, vol. 1, 2003, pp. 175-192.DOI: 10.1016/S1570-8705(03)00019-2.

[2] Oscar F. Gonzalez, Michael Howarth, George Pavlou, "Detection of Packet Forwarding Misbehavior in Mobile Ad-Hoc networks", Journal of Internet Engineering, vol. 2, issue. 1, 2008.

[3] H. Yang, J. Shu, X. Meng, and S. Lu, "SCAN: Self-organized network-layer security in mobile ad hoc networks," IEEE Journal on Selected Areas in Communications, vol. 24, No 2, FEB' 2006, pp. 261-273.

[4] Khurana, S.; Gupta, N.; Aneja, N, "Minimum Exposed Path to the Attack (MEPA) in Mobile Ad Hoc Network (MANET)", 6th International Conference on Networking (ICN'07), April 2007, pp: 16.

[5] Ming Yu; Mengchu Zhou; Wei Su, "A Secure Routing Protocol Against Byzantine Attacks for MANETs in Adversarial Environments", IEEE Transactions on Vehicular Technology, Volume 58, Issue 1, Jan 2009, pp: 449 – 460.

[6] Y. Hu,A. Perrig,and D.Johnson, Ariadne: A Secure On-Demand Routing for AdHocNetworks. Proc.of Mobicom 2002, Atlanta, 2002.

[7] Durgesh Wadbude, Vineet Richariya," An Efficient Secure AODV Routing Protocol in MANET", International Journal of Engineering and Innovative Technology (IJEIT) Volume 1, Issue 4, April 2012, pp. 274 – 279.

[8] M. Rajesh Babu et al., An Energy Efficient Secure Authenticated Routing Protocol for Mobile Ad hoc Networks. International Journal of Reviews in Computing, Vol. 7, Sep. 2011.

Cite this article as: P Vigneshwaran, R Dhanasekaran. "Hash based Secure Multicast Routing in Mobile Ad Hoc Network." *International Conference on Interdisciplinary Research in Electronics and Instrumentation Engineering (2015)*: 55-60. Print.

[9] Poonam Yadav, Rakesh Kumar Gill, Naveen Kumar, A Fuzzy Based Approach to Detect Black Hole Attack, International Journal of Soft Computing and Engineering (IJSCE) ISSN: 2231-2307, Volume-2, Issue-3, Jul. 2012.

[10] Feng He et al., S-MAODV: A Trust Key Computing Based Secure Multicast Ad-hoc On Demand Vector Routing Protocol, 3rd IEEE International Conference on Computer Science and Information Technology, Jul. 2010.

[11] R. Kalpana et al., Mobile Anonymous Trust Based Routing Using Ant Colony Optimization, IEEE Asia-Pacific Services Computing Conference (APSCC), 2010.

[12] Mike Burmester et al., "Towards provable security for route discovery protocols in mobile ad hoc networks", Global Information Infrastructure Symposium (GIIS), 2011, Aug. 2011.

[13] Stefaan Seys et al., ARM: Anonymous Routing Protocol for Mobile Ad hoc Networks, International Symposium on Computer Networks and Distributed Systems (CNDS), Feb. 2011.

[14] K.Seshadri Ramana et al., A Trust-Based Secured Routing Protocol for Mobile Ad hoc Networks. , International Conference on Recent Trends in Information Technology, (ICRTIT), Apr.2012.

[15] Sridhar Subramanian et al., Trust Based Scheme for QoS Assurance in Mobile Ad-Hoc Networks, Second International Conference on Digital Information and Communication Technology and It's Applications (DICTAP) May 2012.

[16] P Vigneshwaran, Dr. R Dhanasekaran, "A Dynamic Approach for Anomaly Detection in AODV", International Journal of Ad hoc, Sensor & Ubiquitous Computing, vol.2, no.4, 2011, pp. 97-105. DOI:10.5121/ijasuc.2011.2408

[17] P Vigneshwaran, Dr. R Dhanasekaran, "Secure Multicast Routing in Mobile Ad Hoc Network Using Secret Sharing", International Journal of Computer Science & Information Technology Advanced Research, vol. 2, SP-1, 2014, pp. 147-150.

[18] P Vigneshwaran, Dr. R Dhanasekaran, "An Intelligent Anomaly Detection for Multicast Routing in Mobile Ad Hoc Network", International Journal of Applied Engineering Research, vol. 10, no. 55, 2015, pp. 2254-2260.

Cite this article as: P Vigneshwaran, R Dhanasekaran. "Hash based Secure Multicast Routing in Mobile Ad Hoc Network." *International Conference on Interdisciplinary Research in Electronics and Instrumentation Engineering (2015)*: 55-60. Print.